CLAIMS

1. In a telecommunications system coupled to a user's telecommunications device, a security apparatus comprising:

a database storing at least one user profile, wherein the profile indicates one of a plurality of security modes selectable by the user; and

a computer coupled to communicate with the database, and coupled to the telecommunications system to receive telecommunications data transmissions, wherein the computer is configured to:

receive mode selection user input, wherein the mode selection user input includes selecting one of the plurality of security modes, wherein the selected security mode is not a personal identification number (PIN) change,

store the selected security mode in the at least one user profile, wherein the user profile corresponds to the user,

in response to a telecommunications call from the user, retrieve the at least one user profile,

receive authorization user input, and

provide user authorization by comparing the received authorization user input to a security code based on the retrieved user profile, wherein the security code is an automatically and dynamically generated user security code based on the selected security mode.

2. The security apparatus of claim 1, wherein the user input is DTMF input provided by a user, and wherein the computer is further configured to:

receive input from the user for assigning a high security mode selected from the plurality of security modes to at least one event, wherein the event is a predetermined time period, a data type received by the telecommunications system or a source of an incoming data signal to the telecommunications system;

periodically generate a user security code; and provide an indication to the user of the user security code, wherein the indication to the user is performed via a paging network.

3. A The security apparatus of claim 1 wherein the plurality of security modes includes a current time sequence recognition mode wherein the user security code is based on predetermined numerical sequence based on an hour of day, day of week, day of month and month of year, and wherein the mode selection user input includes a user selected arrangement of the hour of day, day of week, day of month and month of year. A

4. The apparatus of claim 1 wherein the plurality of security modes includes a personal question response recognition mode wherein the computer is further configured to:

retrieve at least a subset of answers to questions stored by the user in the user security record;

receive answers to a plurality of questions answerable by the user;

randomly shuffle an order of the plurality of questions and providing the shuffled questions to the user; and

receive user input answers corresponding to the answers to the plurality of questions in the shuffled order, wherein the user security code corresponds to the answers in the shuffled order.

5. A method of providing security for a system, comprising:

receiving user input;

retrieving a user profile, wherein the profile indicates one security mode; and

providing authorization by comparing the received user input to a security code based on the retrieved user profile, wherein the security code is an automatically and dynamically generated user security code.

6. The method of claim 5 wherein the system is a telecommunications system, wherein the user input is DTMF input provided by a user, and wherein the method includes:

receiving input from the user for assigning a high security mode selected from a plurality of security modes to at least one event, wherein the selected security mode is not a personal identification number (PIN) change, and wherein the event is a predetermined time period, a data type received by the telecommunications system or a source of an incoming data signal to the telecommunications system; and

providing an indication to the user of the user security code, wherein the user security code is periodically generated, and wherein the indication to the user is performed via a paging network.

7. The method of claim 5 wherein the system is a telecommunications system, and wherein the method includes:

receiving input from the user for assigning a selected security mode selected from a plurality of security modes to at least one event, wherein the event is a predetermined time, a data type received by the telecommunications system or a source of an incoming data signal to the telecommunications system; and wherein the predetermined time is a time of day or day of week, wherein the data type is a voice telephone call, videophone call, electronic mail transmission or a facsimile transmission, and wherein the source is an internal/external transmission or a transmission from a predetermined source.

8. The method of claim 5 wherein the system is a telecommunications system, and wherein the user input is DTMF data, voice pattern fingerprint data, voice recognized command data, alphanumeric data or bitmap data.

9. The method of claim 5 wherein the method includes:

receiving input from the user for assigning a selected security mode selected from a plurality of security modes to at least one event, wherein the event is a predetermined time, a data type received by the system, or a source of an incoming data signal to the system.

10. The method of claim 5 wherein the system is a telecommunications system, and wherein the user input is DTMF data, voice pattern fingerprint data, voice recognized command data, alphanumeric data or bitmap data.

11. The method of claim 5 wherein providing authorization includes providing authorization to the user to access stored data files.

12. The method of claim 5 wherein providing authorization includes providing authorization to the user to access facilities.

13. The method of claim 5 wherein the system is a telecommunications system, and wherein the at least one security mode includes a security algorithm that generates a user security code, wherein the user knows the security algorithm and may approximately concurrently generate the same user security code.

14. The method of claim 5, further comprising communicating to the user which of a plurality of security modes is an indicated security mode.

15. The method of claim 5, further comprising;

encrypting a received telecommunication transmission, and .

receiving a decryption code from the user to decrypt the received telecommunication transmission.

16. The method of claim 5, further comprising providing an indication to the user of the user security code, wherein the user security code is periodically generated, and wherein the indication to the user is performed via an email transmission.

17. The method of claim 5 wherein the security mode includes automatically and periodically generated user security code recognition and wherein the method includes:

providing an indication to the user of the user security code, wherein the user security code is periodically generated, and wherein the indication to the user is performed via a paging network.

18. The method of claim 5, further comprising a plurality of security modes, including a voice pattern profile recognition mode.

19. A The method of claim 5 wherein the security mode includes a current time sequence recognition mode wherein the user security code is based on predetermined numerical sequence based on a hour of day, day of week, day of month and month of year, and wherein the hour of day, day of week, day of month and month of year are arranged in a predetermined fashion known by the system and the user.

20. The method of claim 5 wherein the security mode includes a personal question response recognition mode wherein the personal question response recognition mode includes:

receiving answers to a plurality of questions answerable by the user;

randomly shuffling an order of the plurality of questions and providing the shuffled questions to the user; and

receiving user input corresponding to the answers to the plurality of questions in the shuffled order, wherein the user security code corresponds to the answers in the shuffled order.

21. A method of providing security for a system, comprising:

receiving user input selecting one of a plurality of security modes, wherein the selected security mode is not a personal identification number (PIN) change;

storing the selected security mode in a user profile, wherein the user profile corresponds to the user; and providing authorization by comparing a received user input to a dynamic security code based on the stored user profile and the user selected security mode.

22. The method of claim 21 wherein the system is a telecommunications system, wherein the user input is DTMF input provided by a user, wherein the dynamic security code is an automatically and dynamically generated user security code based on the selected security mode, and wherein the method includes:

receiving input from the user for assigning a high security mode selected from the plurality of security modes to at least one event, wherein the event is a predetermined time period, a data type received by the telecommunications system or a source of an incoming data signal to the telecommunications system; and

providing an indication to the user of the user security code, wherein the user security code is periodically generated, and wherein the indication to the user is performed via a paging network.

23. The method of claim 21 wherein the system is a telecommunications system, and wherein the method includes:

receiving input from the user for assigning a selected security mode selected from the plurality of security modes to at least one event, wherein the event is a predetermined time, a data type received by the telecommunications system or a source of an incoming data signal to the telecommunications system; and wherein the predetermined time is a time of day or day of week, wherein the data type is a voice telephone call, videophone call, electronic mail transmission or a facsimile transmission, and wherein the source is an internal/external transmission or a transmission from a predetermined source.

24. The method of claim 21 wherein at least one of the plurality of security modes includes a security algorithm that generates the dynamic security code, wherein the user knows the security algorithm and may approximately concurrently generate the same dynamic security code.

25. The method of claim 21, further comprising;

encrypting a received telecommunication transmission with the dynamic security code.

26. The method of claim 21, further comprising providing an indication to the user of the dynamic security code, wherein the dynamic security code is periodically generated, and wherein the indication to the user is performed via an email or pager transmission.

27. The method of claim 21 wherein the plurality of security modes includes a current time sequence recognition mode wherein the dynamic security code is based on predetermined sequence based on a hour of day, day of week, day of month and month of year, and wherein the hour of day, day of week, day of month and month of year are arranged in a predetermined fashion by the method and known by the user.

28. The method of claim 21 wherein the plurality of security modes includes a personal question response recognition mode wherein the personal question response recognition mode includes:

receiving answers to a plurality of questions answerable by the user;

randomly shuffling an order of the plurality of questions and providing the shuffled questions to the user; and

receiving user input corresponding to the answers to the plurality of questions in the shuffled order, wherein the user security code corresponds to the answers in the shuffled order.

29. The method of claim 21 wherein the user selected security mode is a randomly applied one of the plurality of security modes, and wherein the method further comprising communicating to the user which of the plurality of security modes is a currently applied security mode.

30. An apparatus for restricting access to one or more resources, the apparatus comprising:

a computer logically coupled to the one or more resources, wherein the computer is configured to receive user input; retrieve a user profile, wherein the profile indicates at least one security mode; automatically and dynamically generate a user security code based on the indicated security mode and the retrieved user profile; and provide authorization by comparing the received user input to the dynamically generated user security code.

31. The apparatus of claim 30 wherein the computer is configured to receive input from the user for assigning a selected security mode selected from a plurality of security modes to at least one event, wherein the event is a predetermined time, a data type received by the telecommunications system or a source of an incoming data signal to the telecommunications system.

32. The apparatus of claim 30 wherein the resources are telecommunications resources, wherein the computer is coupled to a telecommunications network, and wherein the at least one security mode includes a security algorithm that generates a user security code, wherein the user knows the security algorithm and may approximately concurrently generate the same user security code.

33. The apparatus of claim 30 wherein the computer is configured to periodically generate the user security code and to provide an indication to the user of the user security code via a computer network or pager network transmission.

34. A The apparatus of claim 30 wherein the security mode includes a current time sequence recognition mode wherein the user security code is based on predetermined numerical sequence based on a hour of day, day of week, day of month and month of year, and wherein the hour of day, day of week, day of month and month of year are arranged in a predetermined fashion known by the computer and the user.

35. The apparatus of claim 30 wherein the security mode includes a personal question response recognition mode wherein the computer is further configured to receive answers to a plurality of questions answerable by the user; randomly shuffle an order of the plurality of questions and providing the shuffled questions to the user; and receive user input corresponding to the answers to the plurality of questions in the shuffled order, wherein the user security code corresponds to the answers in the shuffled order.

36. An apparatus for providing security for a system, the apparatus comprising:

means for receiving user input selecting one of a plurality of security modes, wherein the selected security mode is not a personal identification number (PIN) change;

means, coupled to the means for receiving, for storing the selected security mode in a user profile, wherein the user profile corresponds to the user; and

means, coupled to the means for storing, for providing authorization by comparing a received user input to a dynamic security code based on the stored user profile and the user selected security mode.

37. The apparatus of claim 36 wherein at least one of the plurality of security modes includes a security algorithm that generates the dynamic security code, wherein the user knows the security algorithm and may approximately concurrently generate the same dynamic security code.

38. The apparatus of claim 36, further comprising means for providing an indication to the user of the dynamic security code, wherein the dynamic security code is periodically generated, and wherein the indication to the user is performed via an email or pager transmission.

39. A computer-readable, signal bearing medium storing instructions for a computer for providing security for a system, the instructions comprising:

receiving user input;

retrieving a user profile, wherein the profile indicates at least one security mode; and

providing authorization by comparing the received user input to a security code based on the retrieved user profile, wherein the security code is an automatically and dynamically generated user security code.

40. The computer-readable medium of claim 39 wherein the system is a computer network, and wherein the computer-readable medium is a logical node in the network receiving the instructions.

41. The computer-readable medium of claim 39 wherein the system is a telecommunications system, wherein the user input is generated by a user of a telecommunications device and wherein the at least one security mode includes a security algorithm that generates a user security code, wherein the user knows the security algorithm and may approximately concurrently generate the same user security code.

42. The computer-readable medium of claim 39, further comprising providing an indication to the user of the user security code, wherein the user security code is periodically generated, and wherein the indication to the user is performed via a computer network or pager network transmission, and wherein the computer-readable medium is a memory or database of the computer.

A 43. The computer-readable medium of claim 39 wherein the security mode includes a current time sequence recognition mode wherein the user security code is based on predetermined numerical sequence based on a hour of day, day of week, day of month and month of year, and wherein the hour of day, day of week, day of month and month of year are arranged in a predetermined fashion known by the system and the user.

44. The computer-readable medium of claim 39 wherein the security mode includes a personal question response recognition mode wherein the personal question response recognition mode includes:

randomly shuffling an order of a plurality of questions and providing the shuffled questions to the user; and

receiving user input corresponding to answers to the plurality of questions in the shuffled order, wherein the user security code corresponds to the answers in the shuffled order.

45. The computer-readable medium of claim 39 wherein the security mode includes a personal question response recognition mode wherein the personal question response recognition mode includes standard questions, personalized questions or a combination of standard questions and personalized questions selected and provided to the user, wherein the security code corresponds to answers to the questions.

A 46. The computer-readable medium of claim 39 wherein the instructions include:

receiving user input selecting one of a plurality of scrambling modes, and

providing an indication to the user of an initial code, where the indication is provided to the user over another system that differs from the system; and

wherein receiving user input includes receiving a true security code corresponding to the indicated initial code modified by the user based on the selected mode.

47. The computer-readable medium of claim 39 wherein the security mode includes a matrix security mode, wherein the matrix mode includes:

receiving position indicating signals from a user indicating initial positions;

providing a matrix of random numbers to the user; and

receiving user input corresponding to numbers selected from the provided matrix based on the initial positions, wherein the user's security code corresponds to numbers within the selected positions.

48. A computer-readable and computer-generated data signal transmitted via a transmission medium, the generated data signal permitting a computer system to perform a method of providing security for a system, comprising:

receiving user input selecting one of a plurality of security modes, wherein the selected security mode is not a personal identification number (PIN) change;

storing the selected security mode in a user profile, wherein the user profile corresponds to the user; and

providing authorization by comparing a received user input to a dynamic security code based on the stored user profile and the user selected security mode.

49. The transmitted data signal of claim 48 wherein at least one of the plurality of security modes includes a security algorithm that generates the dynamic security code, wherein the user knows the security algorithm and may approximately concurrently generate the same dynamic security code.

50. The transmitted data signal of claim 48, further comprising;

encrypting a received telecommunication transmission with the dynamic security code.

51. The transmitted data signal of claim 48, further comprising providing an indication to the user of the dynamic security code, wherein the dynamic security code is periodically generated, and wherein the indication to the user is performed via an email or pager transmission.

A 52. The transmitted data signal of claim 48 wherein the plurality of security modes includes a current time sequence recognition mode wherein the dynamic security code is based on predetermined sequence based on a hour of day, day of week, day of month and month of year, and wherein the hour of day, day of week, day of month and month of year are arranged in a predetermined fashion by the method and known by the user.

53. In a system, a user prompt signal for use in providing security for the system, comprising:

a first user prompt portion for instructing a user to select one of a plurality of security modes;

a second user prompt portion for instructing a user to input a modification to a user profile, wherein the user profile corresponds to the user, wherein the modification applies to a user selected security mode, and wherein the selected security mode and modification are not a personal identification number (PIN) change; and

a third user prompt portion for instructing a user to input a dynamic security code based on the modified user profile and the user selected security mode.

54. The user prompt signal of claim 53 wherein the first, second and third user prompt portions are voice scripts transmitted to a user over a telecommunications network.

55. The user prompt signal of claim 53 wherein the first, second and third user prompt portions are display descriptions transmitted to a user over a computer network.

56. The user prompt signal of claim 53 wherein the first user prompt portion includes instructions for instructing a user to select a user interrogation security mode, and wherein the second user prompt portion includes options for selection standard or customized questions for the user interrogation security mode.

A

57. The user prompt signal of claim 53 wherein the first user prompt portion includes selecting one of a plurality of transmitted code scrambling modes corresponding to methods of generating a dynamic security code based on an initial code transmitted to the user.

58. The user prompt signal of claim 53 wherein the first user prompt portion includes instructions for instructing a user to select one of a plurality of positions within an initial matrix, and the third user prompt portion includes instructions for instructing the user

to input the dynamic security code based on the selected positions and a transmitted matrix of random numbers.

59. A method of providing security for a system, comprising:

providing to users a plurality of security modes, wherein the plurality of security modes include modes in addition to personal identification number (PIN) changes, and where at least one security mode has an associated fee higher than a fee associated with other security modes in the plurality of security modes;

storing user selected security modes in respective user security records; and

charging users selecting the at least one security mode with the associated higher fee.

60. The method of claim 59, further comprising charging users a selected fee for being able to employ a plurality of security modes.

61. A computer-readable medium containing a data structure for use in restricting access to resources, the data structure comprising:

at least first and second fields identifying respective first and second user-selectable security modes, wherein the first and second security modes do not both represent a personal identification number (PIN) change, and wherein the first and second security modes each restrict access to the resources; and

at least a third field comprising parameters associated with a user-selected one of the first and second security modes.

62. The computer-readable medium of claim 61 wherein the resources are telecommunications resources, and wherein the data structure includes:

additional fields for user-initiated assigning of a selected security mode selected from the plurality of security modes to at least one event, wherein the event is a predetermined time, a data type received by the telecommunications resources or a source of an incoming data signal from the telecommunications resources.

63. The computer-readable medium of claim 61, further comprising:

an encryption enabled field indicating a received telecommunication transmission is encrypted.

64. The computer-readable medium of claim 61, further comprising email and pager address fields corresponding to a user's email address and pager number respectively, and wherein the first security mode includes providing an indication to the user of the dynamic security code, wherein the dynamic security code is periodically generated, and wherein the indication to the user is performed via an email or pager transmission.

A 65. The computer-readable medium of claim 61 wherein the first security modes includes a current time sequence recognition mode wherein the dynamic security code is based on predetermined sequence based on a hour of day, day of week, day of month and month of year, and wherein the data structure includes fields indicating an order of hour of day, day of week, day of month and month of year variables.

66. In a security system for restricting access to one or more resources, an apparatus comprising:

a pager network component coupled to the security system, wherein the pager network component is configured to receive user security codes periodically and randomly generated by the security system and transmitted to the pager network component, wherein the pager network component is further configured to transmit the user security codes to a plurality of user pager devices, and wherein the user security codes are required for accessing the one or more resources.

67. The apparatus of claim 66 wherein the user security codes are encrypted before the pager network component transmits the user security codes to the plurality of user pager devices.

68. An apparatus for accessing one or more resources whose access thereto is restricted, the apparatus comprising:

a mobile telecommunications device having a wireless transceiver, a user-input device, a user-output device, and a processor coupled to the transceiver and user input and output devices, wherein the processor is configured to provide user identification data to identify a user profile remotely stored at a server; receive user input for a user security code, wherein the security code corresponds to an automatically and dynamically generated user security code generated at the server computer based on the retrieved user profile; and receiving access to one or more resources based on a correlation between the provided user input and the automatically and dynamically generated user security code.